

# EXHIBIT C

**REESE RICHMAN LLP**

Kim E. Richman

[krichman@reeserichman.com](mailto:krichman@reeserichman.com)

Michael R. Reese

[mreese@reeserichman.com](mailto:mreese@reeserichman.com)

875 Avenue of the Americas, 18<sup>th</sup> Floor

New York, New York 10001

Telephone: (212) 643-0500

Facsimile: (212) 253-4272

- and -

**MILBERG LLP**

Sanford P. Dumain

[sdumain@milberg.com](mailto:sdumain@milberg.com)

Peter E. Seidman

[pseidman@milberg.com](mailto:pseidman@milberg.com)

One Penn Plaza

New York, New York 10119

Telephone: (212) 594-5300

Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

★ FILED ★

2012 MAY 25 PM 4:39

CLERK  
U.S. DISTRICT COURT  
E.D.N.Y.  
AFTER HOURS DROP BOX

**CV 12 - 2674**

**SUMMONS ISSUED**

**KUNTZ, J.**

**ORENSTEIN, M.J.**

**UNITED STATES DISTRICT COURT**

**EASTERN DISTRICT OF NEW YORK**

MICHAEL FROHBERG and ANDY WU, on  
behalf of themselves and all others similarly  
situated,

Plaintiffs,

vs.

MEDIA INNOVATION GROUP, LLC and WPP  
PLC,

Defendants.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Michael Frohberg and Andy Wu (collectively, "Plaintiffs") allege the following, based upon personal knowledge and upon information and belief derived from, among other things, investigation of counsel and review of public documents.

### **NATURE OF THE ACTION**

1. This is a class action against Media Innovation Group, LLC ("MIG") and WPP plc ("WPP") (collectively, "Defendants") arising from Defendants' hacking of computers and mobile devices, Defendants' invasion of Internet users' online privacy, and MIG's intentional misrepresentations related to both of these activities.

2. Defendants circumvented the privacy protections on Plaintiffs' Safari<sup>1</sup> web browsers, thereby hacking into Plaintiffs' computers and mobile devices (collectively, "Devices"). Subsequently, Defendants placed cookies on Plaintiffs' Safari browsers that Defendants used to obtain information about Plaintiffs and their Devices as they used Safari to browse web pages to which Defendants delivered web content as a third party. Included in the private information that Defendants obtained in this manner was sensitive, personal, and personally identifiable information, and, as set forth herein, Defendants, without Plaintiffs' knowledge, misappropriated and exploited this private information for their own uses. MIG thereby violated its own privacy policy – *i.e.*, a policy that proudly proclaims MIG's commitment to "protecting the privacy of Internet users." MIG further assured Internet users that adjusting Safari's privacy controls to disallow setting of cookies is an effective way to prevent MIG from collecting information about them as they browse the Internet using Safari. See <http://www.themig.com/en-us/privacy.html> (Under the heading "Information We Collect Through Our [Third Party Advertising] Services", MIG states that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies.").

3. These actions of Defendants violated New York General Business Law § 349; California Penal Code § 502; Article I, Section 1, of the California Constitution; and California

---

<sup>1</sup> All references to "Safari" are to the Safari web browser developed by Apple Inc.

Penal Code § 630 *et seq.* Defendants' conduct also constitutes trespass to personal property / chattels under New York common law, invasion of privacy under California common law, and intentional misrepresentation under New York and California common law.

### **JURISDICTION AND VENUE**

4. This Court has original jurisdiction over this class action under 28 U.S.C. § 1332(d), which, under the provisions of the Class Action Fairness Act ("CAFA"), explicitly provides for the original jurisdiction of the Federal Courts in any class action in which at least 100 members are in the proposed plaintiff class, any member of the plaintiff class is a citizen of a State different from any defendant, and the matter in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs. Plaintiffs allege that the total claims of individual members of the proposed Class are well in excess of \$5,000,000 in the aggregate, exclusive of interest and costs.

5. Venue for this action properly lies in this District pursuant to 28 U.S.C. § 1391. Substantial acts in furtherance of the alleged improper conduct, including hacking of Plaintiffs' and the Class members' Devices, occurred within this District.

### **THE PARTIES**

6. Plaintiff Michael Frohberg resides in New York and uses his Device there. Mr. Frohberg values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Frohberg browses the Internet using the Safari browser on his computer. At all relevant times, Safari's "Third-Party-Blocking Only Option" (described in detail below) was either operating by default or had been selected by Mr. Frohberg. Mr. Frohberg used Safari to visit web pages that included advertisements (the "Hacking Ads", described in detail below) that Defendants used to hack into his Device and, subsequently, to place tracking mechanisms called "cookies" on the Device. Defendants used the cookies so placed (in the case of MIG, a cookie called "id", and in the case of WPP, a cookie called "OAX") to obtain "End User Information" (as defined below) about Mr. Frohberg and his Device as he used Safari to browse web pages to which Defendants delivered web content. In

this manner, Defendants obtained private information about Mr. Frohberg and his Device without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Frohberg mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendants (in the manner described herein), and Mr. Frohberg mistakenly believed that Defendants' Hacking Ads were a benign part of the online environment. When Mr. Frohberg discovered that Defendants had hacked his Device and learned and collected private information about him without his permission, Mr. Frohberg was shocked, humiliated, and angered and he suffered emotional distress. Furthermore, Defendants' conduct undermined Mr. Frohberg's faith and confidence in the trustworthiness and integrity of the Internet. Defendants degraded the value of Mr. Frohberg's Device and deprived him of the ability to sell to Defendants the information that Defendants collected against his will.

7. Plaintiff Andy Wu resides in California and uses his Devices there. Mr. Wu values his online privacy, especially when using the Internet in the seclusion of his home and/or when conducting his personal affairs. Mr. Wu browses the Internet using the Safari browser on both his iPad and computer. At all relevant times, Safari's Third-Party-Blocking Only Option was either operating by default or had been selected by Mr. Wu. Mr. Wu used Safari to visit web pages that included Hacking Ads that Defendants used to hack into his Devices and, subsequently, to place the "id" and "OAX" cookies on the Devices. Defendants used the cookies to obtain End User Information about Mr. Wu and his Devices as he used Safari to browse web pages to which Defendants delivered web content. In this manner, Defendants obtained private information about Mr. Wu and his Devices without his permission and against his will (as expressed by means of Safari's Third-Party-Blocking Only Option). Mr. Wu mistakenly believed that Safari's privacy controls protected him from having his information obtained by Defendants (in the manner described herein), and Mr. Wu mistakenly believed that Defendants' Hacking Ads were a benign part of the online environment. When Mr. Wu discovered that Defendants had hacked his Devices and learned and collected private information about him without his permission, Mr. Wu was shocked, humiliated, and angered and he suffered emotional

distress. Furthermore, Defendants' conduct undermined Mr. Wu's faith and confidence in the trustworthiness and integrity of the Internet. Defendants degraded the value of Mr. Wu's Devices and deprived him of the ability to sell to Defendants the information that Defendants collected against his will. (Exhibit 1 hereto shows the results of a diagnostic test performed on Mr. Wu's iPad through the website of the Network Advertising Initiative, a self-regulatory organization comprised of over 80 online advertising companies, including MIG.).

8. Defendant Media Innovation Group, LLC is an advertising technology provider within the WPP family of companies. MIG is a Delaware limited liability company that maintains its corporate headquarters at 132 West 31st Street, 12th Floor, New York, New York 10001. See <http://www.wpp.com/wpp/companies/officedetail.htm?id=6212>. MIG conducts business throughout New York, the nation, and internationally.

9. Defendant WPP plc is a public limited company that maintains its principal executive office in Dublin, Ireland, and its main management office in London, United Kingdom. WPP has an office in New York, New York, and owns MIG. WPP is a foreign private issuer registered with the Securities and Exchange Commission as WPP plc, and is traded on the NASDAQ as WPPGY. WPP conducts business throughout New York, the nation, and internationally.

#### **STATEMENT OF THE CASE**

10. People have incorporated the web into their personal lives, through the use of things like social media, dating sites, digital commerce, political forums, and sites containing medical information. See The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012) (Foreword).

11. Plaintiffs at all relevant times used the Internet to communicate with others via social media, to engage in commerce, and to search for a wide variety of information, much of it personal, sensitive, and private. They often browsed the Internet from the seclusion of their homes and at all relevant times did not expect, nor did they have any reason to expect, that outsiders would observe or record their online activities.

12. This expectation derived, in part, from various mechanisms that are designed to grant Plaintiffs control over who may access information about them and their Devices as they browse the Internet.<sup>2</sup> These mechanisms include the privacy controls incorporated into Apple Inc.'s Safari web browser (the "Privacy Controls").<sup>3</sup> Safari's Privacy Controls are adjustable at the discretion of the Safari user. At all relevant times, Plaintiffs had available a choice:

- (a) They could keep their "End User Information" (as defined below) secret from all websites.
- (b) They could keep their End User Information secret from all websites except for the websites whose web pages they visited (the "First Party Content Providers"). For example, if a Safari user chose this option and then visited a web page on the site located at <http://www.amazon.com/> ("amazon.com"), Safari would allow amazon.com to set cookies on the Safari user's Device.<sup>4</sup> If amazon.com then set a cookie(s) on the user's Device, amazon.com could use the cookie(s), among other things, to facilitate collection of End User Information about the Safari user whenever the user visited web pages that included content provided by amazon.com,<sup>5</sup> to streamline the purchase process, or to facilitate

---

<sup>2</sup> The "Do Not Track" system, which allows consumers to signal to online companies that they do not want to be tracked, is one such mechanism. See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* i, iii, v (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.

<sup>3</sup> The Privacy Controls only protect Internet users when they are browsing using Safari. The Privacy Controls have no effect on and cannot protect browsing conducted using other web browsers, such as Windows Internet Explorer (developed by Microsoft Corporation) or Mozilla Firefox (developed by Mozilla Foundation and Mozilla Corporation).

<sup>4</sup> In this instance, amazon.com is the website acting as the First Party Content Provider.

<sup>5</sup> Practically speaking, a website cannot efficiently and reliably collect End User Information about an Internet user without setting a cookie on the Internet user's Device.

recommendation of products based on the user's amazon.com browsing and purchase history. Many Internet users are willing to allow First Party Content Providers to set cookies (and thereby potentially to obtain End User Information about them) because many web pages cannot function properly (or in some cases, at all) if the First Party Content Provider cannot set cookies. This option is the default option in Safari's Privacy Controls – *i.e.*, it is the one that is operational by default and remains in operation unless the Safari user switches to another option. Herein, this option is referred to as the “Third-Party-Blocking Only Option.”

- (c) They could allow not only First Party Content Providers but also “Third Party Content Providers” to set cookies on their Devices and thereby potentially obtain End User Information about them as they browse the web using Safari. A “Third Party Content Provider” is a website that delivers content to a web page that is part of a separate, different website, as an Internet user is visiting the page.<sup>6</sup> For example, when an Internet user is visiting a web page on the site located at <http://www.facebook.com/> (“facebook.com”), the web page may include content (for example, an ad) delivered from the site located at <http://www.third-party-advertiser.com/> (“third-party-advertiser.com”). In this instance, facebook.com is acting as a First Party Content Provider and third-party-advertiser.com is acting as a Third Party Content Provider. Herein, the content delivered by a Third Party Content Provider to a First Party Content Provider's web page is called “Third Party Content.”<sup>7</sup>

---

<sup>6</sup> The latter website is thus acting as a First Party Content Provider.

<sup>7</sup> Examples of Third Party Content include advertisements and “web beacons” (further explained herein).



13. A Safari user who has selected the Third-Party-Blocking Only Option can stop the Privacy Controls from keeping End User Information secret from a specific Third Party Content Provider by submitting an online form to that Third Party Content Provider (the "Form Exception").

14. As used herein, the term "End User Information" means information that a website can obtain about an Internet user after the site has set a cookie on the user's Device. The information may be obtained when the user visits either (i) a web page that is part of the site or (ii) a web page to which the site is delivering Third Party Content. End User Information includes but is not limited to the Uniform Resource Locator ("URL") of the page that the user visited (i) on the site or (ii) to which the site delivered Third Party Content; the time at which the user visited the page; details about the operating system on which the user's browser was running (for example, "Mac OS X" on an iPad); and details about the user's web browser (including information about extensions added to the browser). If a site sets a cookie on an Internet user's Device and the user subsequently visits a series of web pages that (i) are part of the site or (ii) are pages to which the site delivers Third Party Content, then the site can collect a list or a history of information about the user (including the information listed in this paragraph).

15. A website can thus collect End User Information about an Internet user when it provides Third Party Content to other sites throughout the web that the user visits, so long as the website has set a cookie on the user's browser. As noted in footnote 7, *supra*, Third Party Content includes but is not limited to ads and "web beacons." "Web beacons" are pieces of web content that are invisible (or extremely small).<sup>8</sup> When a website delivers a web beacon to a web page as Third Party Content, the Internet user visiting the page is almost always unaware that the web beacon is included on the page (unlike the case where an ad is delivered to a web page as

---

<sup>8</sup> Web beacons are alternatively known as "web bugs", "tags", "tracking pixels", "1 x 1 gifs", and "clear gifs". Upon information and belief, MIG's privacy policy refers to web beacons as "pixels." See <http://themig.com/en-us/privacy.html> ("We collect Non-PII through the use of cookies, pixels and related technology.").

Third Party Content). The purpose, however, of delivering a web beacon as Third Party Content to a web page is not for the Internet user visiting the page to see the web beacon. It is instead to allow the site delivering the web beacon to obtain End User Information about the user (which is, practically speaking, only possible when the Third Party Content Provider has set a cookie on the user's Device).

16. Few Internet users are willing to allow websites they have never directly visited to obtain End User Information about them, even if those sites have delivered Third Party Content to (first party) web pages that the users have visited.

17. Defendants' business includes delivering ads as Third Party Content to web pages throughout the World Wide Web on behalf of Defendants' advertiser clients.

18. Defendants' business also includes obtaining End User Information about Internet users as the users browse sites to which Defendants deliver Third Party Content (including ads and web beacons), which is possible when Defendants have set cookies on the Internet users' Devices.

19. Defendants used computer programming language contained in some of the ads they delivered to web pages as Third Party Content (the "Hacking Ads") to disable the protection provided by Safari's Privacy Controls – the Safari users' express preference with regard to setting of cookies on their Devices, including cookies used to obtain End User Information – with respect to Defendants. *See infra* ¶ 12.

20. Specifically, when Defendants delivered a Hacking Ad as Third Party Content to a web page that was loading in a Plaintiff's or Class member's Safari browser, the computer programming language within the Hacking Ad caused the browser to *immediately* send an *invisible* online form back to Defendants, triggering Safari's Form Exception with respect to Defendants (*i.e.*, turning off Safari's privacy protections with respect to Defendants).

21. However, a Safari user is the only appropriate person to fill out and send this type of online form from the user's Device to Defendants, especially when doing so has the effect of

disabling Safari's privacy protections with respect to Defendants. Defendants thus hacked Plaintiffs' and the Class members' Devices by means of the Hacking Ads.

After Defendants had hacked Plaintiffs' and the Class members' Devices, Safari's Privacy Controls no longer prevented Defendants from setting cookies on Plaintiffs and the Class members' Devices, including cookies that Defendants could use in conjunction with Third Party Content (as described above) to obtain End User Information about Plaintiffs and the Class members. Specifically, once Defendants had triggered Safari's Form Exception, Defendants were able to and did place a cookie used by MIG and a cookie used by WPP on the Device that was hacked.

22. The cookie that MIG placed was called "id". Each "id" cookie contains an ID that MIG uses for tracking purposes in its "Zeus Advertising Platform" ("ZAP"). ZAP analytics is a tool that provides Internet user data and analysis that enables third party advertisers to serve ads that are tailored to the Internet user's preferences as revealed, in significant part, through their private Internet browsing history. ZAP provides "a holistic view of site analytics and campaign data for a comprehensive understanding of every individual consumer" and collects and stores "over 13 months of historical user-level data and draws from it to provide complex and robust analysis." See [http://www.netezza.com/documents/MIG\\_CaseStudy.pdf](http://www.netezza.com/documents/MIG_CaseStudy.pdf) (case study on MIG prepared by Netezza Corporation).<sup>9</sup> With ZAP, "MIG is currently tracking the effectiveness of every single advertising element within many live campaigns that reach hundreds of millions of unique users per month...." See *id.*

23. The cookie that WPP placed was called "OAX". Each "OAX" cookie contains an ID that WPP uses for tracking purposes with its "B3" product. "B3" is an "ad optimization product" developed by WPP, GroupM (a WPP subsidiary), MIG, and Compete (a Kanter Media company). See <http://www.wpp.com/wpp/press/press/default.htm?guid={bcf57ca0-dbc0-4329-8410-2a0c876adea0}>. According to WPP's website, B3 is the "the leading agency tool for

---

<sup>9</sup> Netezza Corporation ("Netezza") designs and markets appliances that house databases, as well as software that analyzes and reports on databases. Netezza technology powers the Zeus Advertising Platform. See [http://www.netezza.com/documents/MIG\\_CaseStudy.pdf](http://www.netezza.com/documents/MIG_CaseStudy.pdf).

acquiring and optimizing display advertising.” See <http://www.wpp.com/wpp/companies/companydetail.htm?id=565>.

24. Stanford researcher Jonathan Mayer first identified Defendants’ Hacking Ads. Mr. Mayer’s blog describes these findings in detail. See <http://webpolicy.org/2012/02/17/safari-trackers/>. Subsequently, Ashkan Soltani, technology adviser for *The Wall Street Journal*, independently confirmed Mr. Mayer’s findings. Mr. Soltani surveyed the top 100 most popular websites as ranked by Quantcast in February 2012.

25. On February 17, 2012, *The Wall Street Journal* published an article describing Mr. Mayer’s and Mr. Soltani’s findings in detail. See Julia Angwin & Jennifer Valentino-Devries, *Google’s iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*, Wall St. J., Feb. 17, 2012, available at <http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html>.

26. Mr. Mayer discovered Defendants’ Hacking Ads on the following sites:  
<http://www.accuweather.com/>  
<http://www.businessinsider.com/>  
<http://www.guardiannews.com/>  
<http://www.sidereel.com/>  
<http://www.tvguide.com/>

27. At all relevant times, Plaintiffs were unaware that Defendants had improperly disabled their Safari privacy protections to allow Defendants to collect and exploit End User Information about them, including their private Internet browsing history.

28. To prevent this, Plaintiffs and the Class members could have deleted the “id” and “OAX” cookies or visited certain websites and opted out of tracking by Defendants. Plaintiffs and the Class members, however, did not know that the “id” and “OAX” cookies were on their Devices or that Defendants were obtaining End User Information about them as they surfed the web. Plaintiffs and the Class members instead believed that Safari’s Privacy Controls, which were set to the Third-Party-Blocking Only Option, prevented Third Party Content Providers (including Defendants when they were acting as a Third Party Content Provider) from placing cookies on their Devices and obtaining End User Information about them. Plaintiffs and the

Class members therefore had no reason to locate and delete the “id” and “OAX” cookies or to attempt to discover which websites they could use to opt out of tracking by Defendants.

29. Defendants injured Plaintiffs and the Class members by hacking their Devices.

30. As a result of being hacked, the Devices no longer functioned as they normally should have.

31. By hacking the Devices and impairing their functionality, Defendants degraded their value.

32. Upon discovering that Defendants had hacked their Devices and obtained private End User Information about them without their permission and against their will (as expressed by means of Safari’s Third-Party-Blocking Only Option), Plaintiffs and the Class members were shocked, humiliated, and angered, and suffered emotional distress.

33. By the above actions, Defendants undermined Plaintiffs’ and the Class members’ confidence in the safety and trustworthiness of the digital environment.

#### **The Value of People’s Personal Information**

34. The personal information that Defendants collected is an asset that is priced, bought, and sold in discrete units for marketing and other purposes. “Websites and stores can . . . easily buy and sell information on valued visitors with the intention of merging behavioral with demographic and geographic data in ways that will create social categories that advertisers covet and target with ads tailored to them or people like them.” Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 29, 2009), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1478214](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214). The more information that is known about a consumer, the more a company will pay to deliver a precisely targeted advertisement to him or her. See Federal Trade Commission (FTC), Protecting Consumer Privacy in an Era of Rapid Change, Preliminary Staff Report (Dec. 2010) (“FTC Report”), at 24.

35. Personal data is viewed as currency. “In many instances, consumers pay for free content and services by disclosing their personal information,” according to former FTC commissioner Pamela Jones Harbour. FTC Roundtable Series 1 on: Exploring Privacy (Matter

No. P095416) (Dec. 7, 2009), at 148, available at [http://www.ftc.gov/bcp/workshops/privacyroundtables/](http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Dec_2009_Transcript.pdf)

PrivacyRoundtable\_Dec\_2009\_Transcript.pdf. In *Property, Privacy, and Personal Data*, Professor Paul M. Schwartz wrote:

Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from this trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information.

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2056-57 (2004).

36. On February 28, 2011, *The Wall Street Journal* highlighted a company called “Allow Ltd.,” which is one of nearly a dozen companies that offers to sell people’s personal information on their behalf and which gives its users 70% of such sales. See Julia Angwin & Emily Steel, *Web’s Hot New Commodity: Privacy*, Wall St. J., Feb. 28, 2011, available at <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html>. For example, one Allow Ltd. user received a payment of \$8.95 for letting Allow tell a credit card company the user was shopping for a new credit card. *Id.*

37. On February 15, 2012, *The Financial Times* acknowledged the value of personal information in the Internet age in the context of Facebook, Inc.’s upcoming initial public offering: “Two weeks ago Facebook announced an initial public offering that could value the company at up to \$100bn. Facebook is worth so much because of the data it holds on its 845m users.”<sup>10</sup>

38. As noted in *The Wall Street Journal*, “[t]rade in personal data has emerged as a driver of the digital economy. Many tech companies offer products for free and get income from online ads that are customized using data about customers. These companies compete for ads, in part, based on the quality of the information they possess about users.” Angwin & Valentino-

---

<sup>10</sup> Richard Falkenrath, *Google Must Remember Our Right to be Forgotten*, Fin. Times, available at <http://www.ft.com/intl/cms/s/0/476b9a08-572a-11e1-869b-00144feabdc0.html#axzz1mgPi5Ux>.



Devries, *Google's iPhone Tracking: Web Giant, Others Bypassed Apple Browser Settings for Guarding Privacy*.

39. Google Inc. ("Google") also acknowledges the value of web browsing histories by purchasing such histories directly from web users. Google's "Screenwise" panel is a program whereby a few thousand Google users are allowing Google to track their web browsing histories in return for up to \$25 in gift cards. See <http://www.google.com/landing/screenwisepanel/>.

40. Defendants ultimately profited from using the information they collected after hacking Plaintiffs' and the Class members' Devices in, among other things, their online advertising business.

41. By the above actions, Defendants deprived Plaintiffs and the Class members of the ability to sell their personal information, including web browsing histories, to Defendants.

**Media Innovation Group, LLC's Intentional Misrepresentations**

42. In its privacy policy, MIG purports to be committed to "protecting the privacy of Internet users" and states that adjusting browser privacy controls to disallow setting of cookies is an effective way to prevent information collection by MIG. See <http://www.themig.com/en-us/privacy.html> (Under the heading "Information We Collect Through Our [Third Party Advertising] Services", MIG states that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies.").

43. However, contrary to MIG's representations, adjusting Safari's Privacy Controls to the Third-Party-Blocking Only Option is completely ineffective at preventing MIG from setting cookies on a Safari user's Device when MIG delivers a Hacking Ad(s) to a web page visited by the Safari user, as detailed herein.

44. Further, MIG's actions, as detailed herein, undercut its purported commitment to protection of people's privacy as they surf the web.

45. MIG's privacy policy further states that MIG is "committed to observing applicable industry guidelines, including those established by the Network Advertising Initiative [("NAI")] and the Interactive Advertising Bureau [("IAB")]" and that MIG is a member of the

NAI and the Digital Advertising Alliance (“DAA”). See <http://www.themig.com/en-us/privacy.html>.

46. The NAI, the IAB, and the DAA all state publicly that web browser privacy controls are an effective means of blocking the setting of cookies. Further, the NAI and the DAA specifically state that use of Safari’s Privacy Controls is an effective means of blocking information collection by Third Party Content Providers. See [http://www.networkadvertising.org/managing/faqs.asp#question\\_13](http://www.networkadvertising.org/managing/faqs.asp#question_13) [the NAI website] (“[To prevent third party tracking using Safari,] you may confirm that your browser is set to accept only first party cookies and do nothing. This default setting will block all third-party cookies, including those of our member ad networks and those of other, non-member ad networks”); <http://www.iab.net/privacymatters/3.php> [the IAB website] (click “Basic Steps” to open a list of “smart precautions”) (“You can manage your cookies by going into your browser’s privacy settings to accept all cookies, no cookies, or save cookies only from sites you know and trust.”); <http://www.aboutads.info/consumers#browsers> [the DAA website] (“Most modern web browsers contain extensive controls that give you the ability to make choices about your privacy. Among other things these controls enable you to block or limit cookies.”; linking to Apple’s page detailing Safari’s capabilities).

47. In spite of MIG’s representation that it observes industry guidelines, MIG’s actions, as detailed herein, fly in the face of industry guidelines. While the NAI, the IAB, and the DAA instruct web users that configuring privacy controls to prevent setting of third party cookies is an effective means of preventing third party information collection, and MIG purports to act in accordance with these instructions, MIG does not in reality act in accordance with these instructions, as detailed herein.

### **CLASS ACTION ALLEGATIONS**

48. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a class of Internet users (collectively, the “Class”) defined as follows:

All Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy



Controls with respect to Defendants, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies. The class period runs from the date that Defendants first began delivering Hacking Ads to web pages to the date of filing of this complaint (the "Class Period").

49. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in New York (collectively, the "New York Subclass") defined as follows:

All New York Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that disabled their Privacy Controls with respect to Defendants, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies; during the Class Period.

50. Plaintiffs also bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of a subclass of Internet users residing in California (collectively, the "California Subclass") defined as follows:

All California Safari users (1) whose Privacy Controls were set to the Third-Party-Blocking Only Option, (2) who visited a web page containing a Hacking Ad that hacked their Privacy Controls, enabling Defendants to place the "id" and "OAX" cookies on the users' Devices, and (3) on whose Devices Defendants then placed the "id" and "OAX" cookies; during the Class Period.

51. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants or any employees, officers, or directors of Defendants; legal representatives, successors, or assigns of Defendants; and any justice, judge or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

52. **Numerosity.** The Class members are so numerous and dispersed nationwide that joinder of all members is impracticable. Upon information and belief, there are millions of Internet users whose Safari Privacy Controls have been debilitated by Defendants' Hacking Ads. The exact number of Class members is unknown, but Plaintiffs reasonably estimate and believe that there are millions of persons in the Class.

53. **Commonality.** There are numerous and substantial questions of law and fact that are common to all members of the Class, which predominate over any question affecting only

individual Class members. The members of the Class were and potentially continue to be subjected to the same practices of Defendants. The common questions and issues raised by Plaintiffs' claims include, *inter alia*, the following:

- (a) whether Defendants hacked Plaintiffs' and the Class members' Devices using Hacking Ads; and
- (b) whether Defendants collected Plaintiffs and the Class members' web browsing histories against their will.

54. **Typicality.** Plaintiffs' claims are typical of the claims of all of the other members of the Class, because their claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendants.

55. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of all members of the Class in the prosecution of this action and in the administration of all matters relating to the claims stated herein. Plaintiffs are similarly situated with, and have suffered similar injuries to, the members of the Class they seek to represent. Plaintiffs have retained counsel experienced in handling class action lawsuits. Neither Plaintiffs nor their counsel have any interest that might cause them not to vigorously pursue this action.

56. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy, since individual joinder of the Class members is impracticable. Even if individual Class members were able to afford individual litigation, it would be unduly burdensome to the Courts in which the individual litigation would proceed. Defendants have subjected the Class to the same violations as referenced herein. Accordingly, class certification is appropriate under Rule 23 because common issues of law and fact regarding Defendants' uniform violations predominate over individual issues, and class certification is a superior method of resolving these claims. No unusual difficulties are likely to be encountered in the management of this action as a class action. Defendants have acted in a manner that affects Plaintiffs and all Class members alike, thereby making appropriate injunctive, declaratory, and other relief appropriate with respect to the Class as a whole.

**CAUSES OF ACTION**

**COUNT ONE**

**(VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349)**

57. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

58. New York General Business Law § 349 prohibits “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state....”

59. In violation of § 349, Defendants engaged in material, deceptive, consumer-oriented acts in the conduct of business that injured Plaintiffs and the Class members.

60. Specifically, Plaintiffs and the Class members mistakenly believed that viewing web pages that included Hacking Ads would not harm their Devices.

61. Defendants’ Hacking Ads appeared to be a non-invasive, benign part of the digital environment.

62. In reality, Defendants used their Hacking Ads to harm Plaintiffs’ and the Class members’ Devices by debilitating the functionality of their Safari Privacy Controls, as described herein.

63. Further, Plaintiffs and the Class members mistakenly believed that Defendants would respect that they, via Safari’s Privacy Controls, had explicitly denied permission to Defendants to use Third Party Content in conjunction with cookies to obtain End User Information about them.

64. In reality, Defendants ignored Plaintiffs’ and the Class members’ explicit prohibition, disabled the functionality of Safari’s Privacy Controls, and used their Third Party Content in conjunction with cookies they set on Plaintiffs’ and the Class members’ Devices to obtain End User Information about Plaintiffs and the Class members as they visited web pages throughout the web.

65. Defendants’ acts and/or omissions were generally aimed at the consuming public.

66. These unlawful deceptive acts directly and proximately caused harm to Plaintiffs and the Class members in the following ways:

- (a) through the degradation in value of their Devices;
- (b) through the loss of their privacy and the exposure of their personal, sensitive, and private information, as a result of which Plaintiffs and the Class members were shocked, humiliated, and angered and suffered emotional distress;
- (c) by depriving Plaintiffs and the Class members of the ability to sell their personal information, including their web browsing histories, to Defendants.

67. As a direct and proximate result of Defendants' violation of § 349, Plaintiffs and the Class members have suffered damages in an amount to be determined at trial.

68. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendants' unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

## **COUNT TWO**

### **(VIOLATION OF THE CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT, CALIFORNIA PENAL CODE § 502)**

69. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

70. California Penal Code § 502(c)(1) prohibits a person from knowingly accessing and without permission altering, damaging, and/or otherwise using data, computers, computer systems, and/or computer networks to:

- (A) execute a scheme or artifice to defraud or deceive, and/or
- (B) wrongfully control or obtain money, property, or data.

71. In violation of § 502(c)(1), Defendants intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to execute a scheme or artifice to defraud or deceive.

72. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices as part of the execution of a scheme in which Defendants intentionally failed to inform Plaintiffs and the Class members that Defendants had hacked their Devices and subsequently used Third Party Content in conjunction with cookies to End User Information about Plaintiffs and the Class members as they surfed the web.

73. In violation of § 502(c)(1), Defendants intentionally and without permission altered, damaged, and otherwise used Plaintiffs' and the Class members' Devices to wrongfully control or obtain money, property, or data.

74. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices without their knowledge to obtain personal data about them, including their web browsing histories. Further, the personal data that Defendants obtained is property.

75. California Penal Code § 502(c)(2) prohibits a person from knowingly accessing and without permission taking, copying, and/or making use of data from a computer, computer system, and/or computer network.

76. In violation of § 502(c)(2), Defendants intentionally and without permission took, copied, and/or made use of data from Plaintiffs' and the Class members' Devices.

77. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices and took information about their web surfing from the Devices, which Defendants made use of in their advertising business.

78. California Penal Code § 502(c)(3) prohibits a person from knowingly and without permission using "computer services" as that term is defined in California Penal Code § 502(b)(4).

79. In violation of § 502(c)(3), Defendants intentionally and without permission used "computer services," including but not limited to storage functions and web history tracking.

80. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Devices, stored cookies on the Devices, and used those cookies in conjunction with browser software on the Devices to obtain End User Information about Plaintiffs and the Class members as they browsed web pages to which Defendants delivered Third Party Content.

81. California Penal Code § 502(c)(4) prohibits a person from knowingly and without permission adding, altering, and/or damaging data, computer software, and/or computer programs that reside and/or exist internal and/or external to a computer, computer system, and/or computer network.

82. In violation of § 502(c)(4), Defendants intentionally and without permission added, altered, and/or damaged data, computer software, and/or computer programs that resided internal to Plaintiffs' and the Class members' Devices.

83. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls, debilitating their functionality.

84. Further, Defendants intentionally and without permission added cookies to Plaintiffs' and the Class members' Devices.

85. California Penal Code § 502(c)(5) prohibits a person from knowingly and without permission disrupting and/or causing the disruption of "computer services" (as that term is defined in California Penal Code § 502(b)(4)) to an authorized user of a computer, computer system, and/or computer network.

86. In violation of § 502(c)(5), as described in detail herein, Defendants disabled the functionality of Plaintiffs' and the Class members' Safari Privacy Controls, thereby disrupting Plaintiffs' and the Class members' desired use of their web browsers and the World Wide Web.

87. California Penal Code § 502(c)(7) prohibits a person from knowingly and without permission accessing computers, computer systems, and/or computer networks.

88. In violation of § 502(c)(7), as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls and placed cookies on their Devices,

which Defendants used in conjunction with Third Party Content to obtain End User Information about them as they surfed the web.

89. California Penal Code § 502(c)(8) prohibits a person from knowingly introducing “computer contaminants” – as defined in California Penal Code § 502(b)(10) – into computers, computer systems, and/or computer networks.

90. In violation of § 502(c)(8), as described in detail herein, Defendants intentionally introduced computer programming code into Plaintiffs’ and the Class members’ Devices that “usurp[ed] the normal operation” of the Devices by hacking Safari’s Privacy Controls, enabling the placement of cookies on the Devices.

91. As a direct and proximate result of Defendants’ violation of California Penal Code § 502, Defendants caused loss to Plaintiffs and the Class members in an amount to be proven at trial.

92. Plaintiffs and the Class members are entitled to recovery of attorneys’ fees pursuant to § 502(e).

93. Plaintiffs and the Class members are entitled to punitive or exemplary damages under California Penal Code § 502(e)(4) because Defendants willfully violated § 502(c) and are guilty of “fraud” as defined by California Civil Code § 3294(c)(3).

94. Under § 3294(c)(3), “fraud” means an intentional misrepresentation, deceit, or concealment of a material fact known to the defendant with the intention on the part of the defendant of thereby depriving a person of property or legal rights or otherwise causing injury.

95. As described in detail herein, Defendants intentionally concealed from Plaintiffs and the Class members the fact that Defendants dismantled the privacy safeguards established by their Privacy Controls.

96. As a result of concealing this fact, Defendants intended to and did deprive Plaintiffs and the Class members of their legal right to privacy.

97. Further, as a result of concealing this fact, Defendants intended to profit and did profit by obtaining without authorization personal, private, and sensitive information about



Plaintiffs and the Class members as they surfed the web and using the information in connection with Defendants' advertising business. Defendants' actions deprived Plaintiffs and the Class of the opportunity to sell the information to Defendants. Defendants thereby deprived Plaintiffs and the Class members of valuable property.

98. Plaintiffs and the Class members have also suffered irreparable injury as a result of Defendants' unlawful conduct, including the unauthorized collection of their personal information. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class members have no adequate remedy at law, entitling them to injunctive relief.

### **COUNT THREE**

#### **(VIOLATION OF ARTICLE I, SECTION 1 OF THE CALIFORNIA CONSTITUTION)**

99. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

100. Article I, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1.

101. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

102. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendants obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.



103. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

104. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

105. Defendants committed a serious invasion of Plaintiffs' and the Class members' privacy interests by hacking their Safari Privacy Controls. Unbeknownst to Plaintiffs and Class members, Defendants made a private decision on behalf of Plaintiffs and the Class members that Defendants were not authorized to make.

106. Defendants committed a serious invasion of Plaintiffs' and the Class members' privacy interests by, after hacking their Safari Privacy Controls, obtaining End User Information (including personal, confidential, and sensitive information) about them as they surfed the web without authorization.

107. By the acts, transactions, and courses of conduct alleged herein, Defendants violated Plaintiffs' and the Class members' inalienable right to privacy.

108. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

#### **COUNT FOUR**

#### **(VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, CALIFORNIA**

#### **PENAL CODE § 630 ET SEQ.)**

109. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

110. In violation of California Penal Code § 631, Defendants, by means of a contrivance (or in "any other manner") made an unauthorized connection, electrically or "otherwise", with the wires, lines, cables, or instruments within the State of California over

which communications or messages traveled between Plaintiffs' and the Class members' web browsers and the websites whose web pages they visited.

111. Specifically, as described in detail herein, Defendants hacked Plaintiffs' and the Class members' Safari Privacy Controls, which enabled them to place cookies on Plaintiffs' and the Class members' devices that they were explicitly not authorized to place. The cookies so placed, when used in conjunction with delivery of Third Party Content to Plaintiffs and the Class members (as described above), enabled Defendants to obtain End User Information about Plaintiffs and the Class members that Defendants would not otherwise have been able to obtain. Accordingly, Defendants created an unauthorized connection to Plaintiffs' and the Class members' communications with the websites whose web pages they visited, which occurred over wires, lines, cables, or instruments within the State of California.

112. In violation of California Penal Code § 631, Defendants willfully, intentionally, without the consent of Plaintiffs and the Class members, and in an unauthorized manner, obtained, read, attempted to read, learned, and/or attempted to learn the contents of Plaintiffs' and the Class members' electronic communications with (or messages to) the websites whose web pages they visited while the communications (or messages) were in transit in or through California and/or while they were being sent from or received at a place within California.

113. Further, websites whose web pages were visited by Plaintiffs and the Class members did not have the authority to consent to alteration by Defendants of Plaintiffs' and the Class members' Safari Privacy Controls.

114. Defendants used and communicated such illegally obtained electronic communications of Plaintiffs and the Class members, including use and communication in their online advertising business.

115. As a direct and proximate result of the above-described conduct by Defendants, Plaintiffs and all Class members have suffered, and, unless such conduct is enjoined, will continue to suffer, damages in an amount to be proven at trial.

116. Pursuant to California Penal Code § 637.2, Plaintiffs and the Class members are entitled to recover three times their actual and/or statutory damages from Defendants, for the conduct described herein.

117. Defendants' conduct is causing, and unless enjoined will continue to cause, Plaintiffs and the Class members great and irreparable injury that cannot be fully compensated for or measured in money. Plaintiffs and the Class members have no adequate remedy at law and, pursuant to California Penal Code § 637.2(b), are entitled to preliminary and permanent injunctions prohibiting further use and communication of their unlawfully obtained information.

#### **COUNT FIVE**

##### **(TRESPASS TO PERSONAL PROPERTY / CHATTELS)**

118. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

119. The common law of New York prohibits the intentional intermeddling with personal property in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

120. In violation of New York common law and as detailed more fully herein, Defendants dispossessed Plaintiffs and the Class members from use and/or access to their Devices, or parts of them, without their knowledge or consent. Further, Defendants' acts constituted an intentional interference with the use and enjoyment of the Devices.

121. Without Plaintiffs' and the Class members' knowledge or consent, Defendants knowingly and intentionally accessed their property and caused them injury.

122. Defendants engaged in deception and concealment in order to gain access to Plaintiffs' and the Class members' Devices.

123. Defendants' hacking of Safari's Privacy Controls and subsequent installation of cookies on Plaintiffs' and the Class members' Devices interfered and/or intermeddled with the Devices, including by altering or damaging controls designed to prevent the information

collection effected by Defendants. Such use, interference, and/or intermeddling was without the knowledge or consent of Plaintiffs and the Class members.

124. Defendants' hacking of Plaintiffs' and the Class members' Devices and subsequent placement of cookies on them impaired their condition and value. In particular, these actions debilitated the functionality of Plaintiffs' and the Class members' Safari Privacy Controls.

125. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and the Class members.

126. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference, and unauthorized access to and intermeddling with Plaintiffs' and the Class members' Devices, Defendants have injured and impaired the condition and value of the Devices as follows:

- (a) By consuming the resources of and/or degrading the performance of Plaintiffs' and the Class members' Devices (including space, memory, processing cycles, and Internet connectivity);
- (b) By diminishing the use of, value, speed, capacity, and/or capability of Plaintiffs' and the Class members' Devices;
- (c) By altering and controlling the functioning of Plaintiffs' and the Class members' Devices;
- (d) By devaluing, interfering with, and/or diminishing Plaintiffs' and the Class members' possessory interest in their Devices;
- (e) By infringing on Plaintiffs' and the Class members' right to exclude others from their Devices;
- (f) By infringing on Plaintiffs' and the Class members' right to determine, as owners of their Devices, which programs should be installed and operated on the Devices, and how programs should be installed and operated on the Devices;

- (g) By compromising the integrity, security, and ownership of Plaintiffs' and the Class members' Devices;
- (h) By forcing Plaintiffs and the Class members to expend time and resources in order to remove the cookies installed on their Devices without notice or consent.

127. Plaintiffs and the Class members have no adequate remedy at law.

### **COUNT SIX**

#### **(INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA COMMON LAW)**

128. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

129. Defendants intruded on Plaintiffs' and the Class members' private affairs and seclusion by hacking their Safari Privacy Controls and placing cookies on their Devices – conduct that Defendants engaged in completely outside of their knowledge and against their express will. The cookies enabled Defendants, without authorization, to obtain End User Information about Plaintiffs and the Class members as they surfed the web, as more fully detailed herein.

130. Plaintiffs and the Class members have a legally protected autonomy privacy interest in making intimate personal decisions regarding the use of their Devices without interference. This interest includes an interest in maintaining the integrity of their web browser privacy controls.

131. Plaintiffs and the Class members have a legally protected privacy interest in the End User Information (including personal, confidential, and sensitive information and web browsing histories) that Defendants obtained by hacking Plaintiffs' and the Class members' Safari Privacy Controls.

132. Plaintiffs and the Class members reasonably expected that they would be able to make intimate personal decisions regarding the use of their Devices free of interference, including decisions related to web browser privacy controls.

133. Plaintiffs and the Class members reasonably expected that their End User Information (including personal, confidential, and sensitive information) and intimate personal decisions would be kept private.

134. Defendants intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by hacking Plaintiffs' and the Class members' Safari Privacy Controls. Unbeknownst to Plaintiffs and the Class members, Defendants made a private decision on behalf of Plaintiffs and the Class members that Defendants were not authorized to make.

135. Defendants intentionally committed a "serious invasion of privacy" that would be highly offensive to a reasonable person by, after hacking Plaintiffs' and the Class members' Safari Privacy Controls, obtaining End User Information about them as they surfed the web without authorization.

136. As a consequence, Plaintiffs and the Class members were personally injured and suffered emotional distress damages.

#### **COUNT SEVEN**

##### **(INTENTIONAL MISREPRESENTATION)**

##### **(AGAINST MEDIA INNOVATION GROUP, LLC, ONLY)**

##### **(NEW YORK SUBCLASS ONLY)**

137. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

138. During the Class Period, MIG engaged in fraudulent, misrepresentative, false, and/or deceptive practices.

139. First, MIG represented to Plaintiffs and the New York Subclass members that MIG was "firmly committed to protecting the privacy of Internet users."

140. MIG made the above representation knowing that MIG was in fact invading Plaintiffs' and the New York Subclass members' online privacy by hacking their Safari Privacy Controls, as detailed herein.

141. Second, under the heading "Information We Collect Through Our [Third Party Advertising] Services" in its privacy policy, MIG represented to Plaintiffs and the New York Subclass members that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies."

142. MIG made the above representation knowing that MIG was in fact delivering Hacking Ads to Plaintiffs and the New York Subclass members as they surfed the web that were specifically designed to and did disable Safari's Third-Party-Blocking Only Option with respect to MIG, allowing MIG to place cookies on Plaintiffs' and the New York Subclass members' Devices, as detailed more fully herein.

143. Third, MIG represented to Plaintiffs and the New York Subclass members that MIG was in compliance with the guidelines of the NAI, the IAB, and the DAA.

144. The websites of the NAI and the DAA explain that Safari's Privacy Controls, when set to block cookies set by websites acting as Third Party Content Providers, are effective at doing so.

145. The IAB's website explains that web browsers' privacy controls, when set to block the setting of cookies, are effective at doing so.

146. While representing that MIG was acting in accord with the policies and representations of the NAI, the IAB, and the DAA, MIG knowingly was delivering Hacking Ads to Plaintiffs and the New York Subclass members as they surfed the web with the specific purpose of disabling Safari's Privacy Controls, setting cookies on their Devices, and obtaining End User Information about them, as detailed herein.

147. These aforementioned frauds, misrepresentations, deceptive, and/or false acts and omissions concerned material facts that were essential to Plaintiffs' and the New York Subclass members' decisions to browse the web using Safari with the Third-Party-Blocking Only Option selected.

148. Plaintiffs and the New York Subclass members would have acted differently had they not been misled, but, instead, had been informed that Safari's Privacy Controls were



ineffective at preventing MIG from setting cookies on their Devices and, using those cookies in conjunction with MIG's Third Party Content, obtaining End User Information about them as they surfed the web.

149. By and through such fraud, deceit, misrepresentations, and/or omissions, MIG intended to induce Plaintiffs and the New York Subclass members to alter their positions to their detriment.

150. Plaintiffs and the New York Subclass members justifiably and reasonably relied on MIG's omissions and misrepresentations, and, as such, were damaged by MIG.

151. As a direct and proximate result of MIG's omissions and misrepresentations, Plaintiffs and the New York Subclass members have suffered damages, including in the following ways:

- (a) On discovering that MIG was hacking their Devices so as to intrude upon their seclusion and observe their personal affairs, as detailed herein, Plaintiffs and the New York Subclass members were shocked, humiliated, and angered, and suffered emotional distress; and
- (b) MIG's intentional misrepresentations enabled MIG to collect Plaintiffs and the New York Subclass members' End User Information (including private, personal, and sensitive information and Safari web browsing histories), thereby depriving Plaintiffs and the New York Subclass members of the ability to sell their End User Information to MIG.

#### **COUNT EIGHT**

##### **(INTENTIONAL MISREPRESENTATION)**

##### **(AGAINST MEDIA INNOVATION GROUP, LLC, ONLY)**

##### **(CALIFORNIA SUBCLASS ONLY)**

152. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.



153. During the Class Period, MIG engaged in fraudulent, misrepresentative, false, and/or deceptive practices.

154. First, MIG represented to Plaintiffs and the California Subclass members that MIG was "firmly committed to protecting the privacy of Internet users."

155. MIG made the above representation knowing that MIG was in fact invading Plaintiffs' and the California Subclass members' online privacy by hacking their Safari Privacy Controls, as detailed herein.

156. Second, under the heading "Information We Collect Through Our [Third Party Advertising] Services" in its privacy policy, MIG represented to Plaintiffs and the California Subclass members that "[a]t all times, you may adjust your computer's web browser settings to refuse all cookies."

157. MIG made the above representation knowing that MIG was in fact delivering Hacking Ads to Plaintiffs and the California Subclass members as they surfed the web that were specifically designed to and did disable Safari's Third-Party-Blocking Only Option with respect to MIG, allowing MIG to place cookies on Plaintiffs' and the California Subclass members' Devices, as detailed more fully herein.

158. Third, MIG represented to Plaintiffs and the California Subclass members that MIG was in compliance with the guidelines of the NAI, the IAB, and the DAA.

159. The websites of the NAI and the DAA explain that Safari's Privacy Controls, when set to block cookies set by websites acting as Third Party Content Providers, are effective at doing so.

160. The IAB's website explains that web browsers' privacy controls, when set to block the setting of cookies, are effective at doing so.

161. While representing that MIG was acting in accord with the policies and representations of the NAI, the IAB, and the DAA, MIG knowingly was delivering Hacking Ads to Plaintiffs and the California Subclass members as they surfed the web with the specific

purpose of disabling Safari's Privacy Controls, setting cookies on their Devices, and obtaining End User Information about them, as detailed herein.

162. These aforementioned frauds, misrepresentations, deceptive, and/or false acts and omissions concerned material facts that were essential to Plaintiffs' and the California Subclass members' decisions to browse the web using Safari with the Third-Party-Blocking Only Option selected.

163. Plaintiffs and the California Subclass members would have acted differently had they not been misled, but, instead, had been informed that Safari's Privacy Controls were ineffective at preventing MIG from setting cookies on their Devices and, using those cookies in conjunction with MIG's Third Party Content, obtaining End User Information about them as they surfed the web.

164. By and through such fraud, deceit, misrepresentations, and/or omissions, MIG intended to induce Plaintiffs and the California Subclass members to alter their positions to their detriment.

165. Plaintiffs and the California Subclass members justifiably and reasonably relied on MIG's omissions and misrepresentations, and, as such, were damaged by MIG.

166. As a direct and proximate result of MIG's omissions and misrepresentations, Plaintiffs and the California Subclass members have suffered damages, including in the following ways:

- (a) On discovering that MIG was hacking their Devices so as to intrude upon their seclusion and observe their personal affairs, as detailed herein, Plaintiffs and the California Subclass members were shocked, humiliated, and angered, and suffered emotional distress; and
- (b) MIG's intentional misrepresentations enabled MIG to collect Plaintiffs and the California Subclass members' End User Information (including private, personal, and sensitive information and Safari web browsing

histories), thereby depriving Plaintiffs and the California Subclass members of the ability to sell their End User Information to MIG.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs and members of the Class seek relief against Defendants as follows:

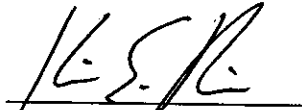
- A. An order certifying that this action is properly brought and may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed as Class Representatives, and that Plaintiffs' counsel be appointed Class Counsel.
- B. Awarding damages as alleged above.
- C. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class members, including, *inter alia*, an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein.
- D. Disgorgement of all revenue earned from selling or otherwise using or trading on the private information obtained from Plaintiffs and the Class members as a result of hacking their Devices, as described herein.
- E. Awarding Plaintiffs and the Class members their reasonable litigation expenses and attorneys' fees; and
- F. Awarding such other and further relief at law or equity as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs and the Class members hereby demand trial of their claims by jury to the extent authorized by law.

DATED: May 25, 2012

**REESE RICHMAN LLP**



Kim E. Richman

[krichman@reese-richman.com](mailto:krichman@reese-richman.com)

Michael R. Reese

[mreese@reese-richman.com](mailto:mreese@reese-richman.com)

875 Avenue of the Americas, 18<sup>th</sup> Floor

New York, New York 10001

Telephone: (212) 643-0500

Facsimile: (212) 253-4272

– and –

**MILBERG LLP**

Sanford P. Dumain

[sdumain@milberg.com](mailto:sdumain@milberg.com)

Peter Seidman

[pseidman@milberg.com](mailto:pseidman@milberg.com)

One Penn Plaza

New York, New York 10119

Telephone: (212) 594-5300

Facsimile: (212) 868-1229

*Attorneys for Plaintiffs and the Proposed Class*

# EXHIBIT 1

If you have any questions, please visit our [FAQ](#) section.

## Opt-Out Status

Select all

Clear

Submit

Member Company	Status	Opt-Out
<b>Adap.tv</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Adblade</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AdBrite</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AdChemy</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Adconion</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Adara Media</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AdMeld</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AddThis</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Aggregate Knowledge</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Akamai</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Akamai (aCerno)</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Aperture</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AppNexus</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>
<b>AudienceScience</b> <a href="#">More Information</a>	<b>No Cookie</b> You have not opted out and you have no cookie from this network.	Opt-Out <input type="checkbox"/>
<b>Batanga (Collective)</b> <a href="#">More Information</a>	<b>Active Cookie</b> You have not opted out and you have an active cookie from this network.	Opt-Out <input type="checkbox"/>



**Batanga (DoubleClick)**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Bizo**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**BlueKai**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**BrightRoll**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Brilig**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Burst Media's adConductor**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Buysight**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Casale Media**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Chango**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Channel Intelligence**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Cognitive Match**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Collective**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Cox Digital Solutions (Adify)**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Cox Digital Solutions (DoubleClick)**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Criteo**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Cross Pixel Media**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**DataLogix**

[More Information](#)

No Cookie

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**DataXu**

[More Information](#)

Active Cookie

You have not opted out and you have an active cookie from this network.

Opt-Out ☐





**Datronics**  
[More Information](#)

**Active Cookie**  
You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Dedicated Networks (AppNexus)**  
[More Information](#)

**Active Cookie**  
You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Dedicated Networks (DoubleClick)**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Dotomi**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Epic Marketplace**  
[More Information](#)

**Active Cookie**  
You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**eXelate Media**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**EZTarget Media**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**FetchBack**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Glam Media**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Google**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**I-Behavior**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Intent Media**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**InterCLICK**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Invite Media**  
[More Information](#)

**Active Cookie**  
You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Kontera**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Legolas Media Inc.**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Lotame**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐

**MAGNETIC**  
[More Information](#)

**No Cookie**  
You have not opted out and you have no cookie from this network.

Opt-Out ☐





**Markit on Demand**  
(formerly Wall Street On Demand)

[More Information](#)

**MaxPoint Interactive**

[More Information](#)

**Media Innovation Group**

[More Information](#)

**MediaMath**

[More Information](#)

**MediaMind**

[More Information](#)

**Mediaplex**

[More Information](#)

**Media6degrees**

[More Information](#)

**Microsoft Advertising**

[More Information](#)

**Mindset Media**

[More Information](#)

**Mixpo**

[More Information](#)

**Netmining**

[More Information](#)

**OwnerIQ**

[More Information](#)

**PubMatic**

[More Information](#)

**Pulse360**

[More Information](#)

**RadiumOne**

[More Information](#)

**Red Aril**

[More Information](#)

**richrelevance**

[More Information](#)

**Rocket Fuel**

[More Information](#)

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**No Cookie**

You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Active Cookie**

You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Rubicon Project**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**ShareThis**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Specific Media**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**SteelHouse**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**TARGUSinfo AdAdvisor**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**33Across**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**TruEffect**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Tumri**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Turn**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**24/7 Real Media**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Undertone Networks**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**ValueClick Media**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Vibrant Media**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**Videology (formerly TidalTV)**  
[More Information](#)

**No Cookie**  
 You have not opted out and you have no cookie from this network.

Opt-Out ☐

**XGraph**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**[x+1] (formerly Poindexter Systems)**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**Yahoo! Ad Network  
 (now including Dapper)**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐

**YuMe, Inc.**  
[More Information](#)

**Active Cookie**  
 You have not opted out and you have an active cookie from this network.

Opt-Out ☐



[More Information](#)

You have not opted out and you have an active cookie from this network.

**Undertone Networks**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**ValueClick Media**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**Vibrant Media**

**No Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have no cookie from this network.

**Videology (formerly TidalTV)**

**No Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have no cookie from this network.

**XGraph**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**[x+1] (formerly Poindexer Systems)**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**Yahoo! Ad Network  
(now including Dapper)**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**YuMe, Inc.**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**AOL Advertising**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

**Tribal Fusion**

**Active Cookie**

Opt-Out ☐

[More Information](#)

You have not opted out and you have an active cookie from this network.

Select all

Clear

Submit

**Opting out of an ad network program using the NAI Opt-out Tool should not affect other services provided by NAI members that rely on cookies, such as email or photo-hosting. [Click here for more information.](#)**

**The NAI has adopted a policy that all NAI member companies set a minimum lifespan of five years for their opt out cookies. [Click here for more information.](#)**

[About Membership](#) | [Members Only Login](#) | [Legal](#)

